

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-232450
(43)Date of publication of application : 16.08.2002

(51)Int.Cl. H04L 12/46
H04L 12/22
H04L 12/66

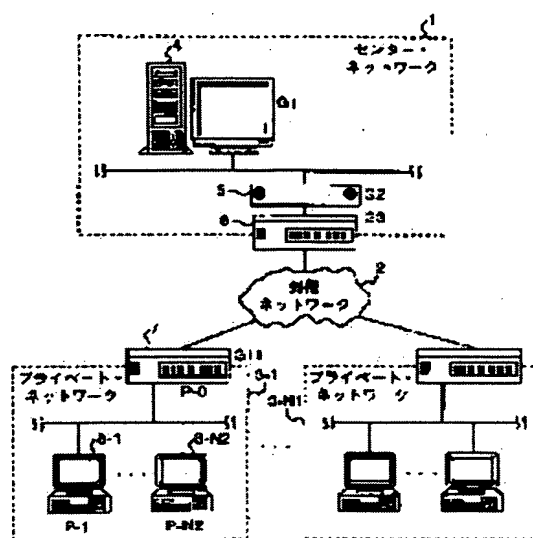
(21)Application number : 2001-024824 (71)Applicant : FURUKAWA ELECTRIC CO LTD:THE
(22)Date of filing : 31.01.2001 (72)Inventor : NANBA MIKAKO

(54) NETWORK REPEATER, DATA COMMUNICATION SYSTEM, DATA COMMUNICATION METHOD AND PROGRAM MAKING COMPUTER PERFORM THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To facilitate the mounting and management of a function performing IPSec communication inside and outside a private network and to reduce the cost.

SOLUTION: A network repeater 7 performs the repeating processing of a packet between the private network 3-1 and an outer network 2, where unique private addresses are used in self-private networks. The repeater has a first repeating part encapsulating an ESP packet transmitted within the private network 3-1 into a UDP packet and repeating it to the outer network 2 and a second repeating part decapsulating the UDP packet from the outer network 2 into the ESP packet and repeating it into the private network 3-1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
H04L 12/46		H04L 12/46	E 5K030
12/22		12/22	5K033
12/66		12/66	B

審査請求 未請求 請求項の数 9 O L (全15頁)

(21) 出願番号 特願2001-24824(P 2001-24824)

(22) 出願日 平成13年1月31日(2001.1.31)

(71) 出願人 000005290

古河電気工業株式会社

東京都千代田区丸の内2丁目6番1号

(72) 発明者 難波 美香子

東京都千代田区丸の内2丁目6番1号 古

河電気工業株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

Fターム(参考) 5K030 GA15 HA08 HD03 HD06 JA05

KA02

5K033 AA08 CB08 CB14 CC01 DA06

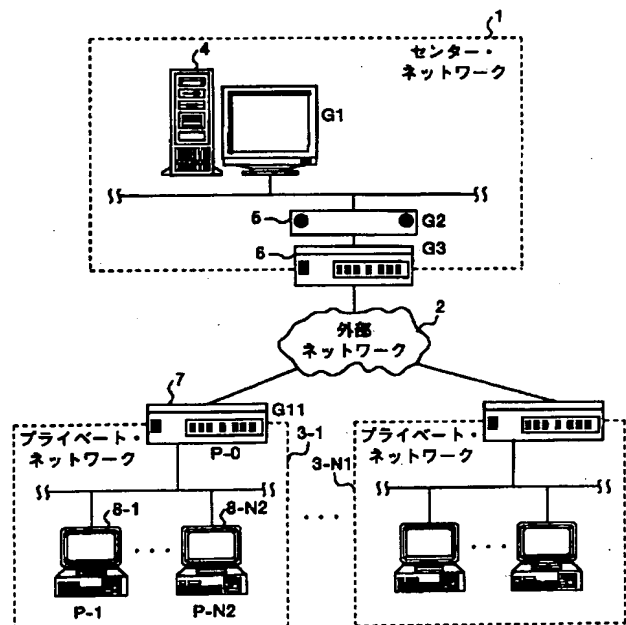
DB13 DB18

(54) 【発明の名称】 ネットワーク中継装置、データ通信システム、データ通信方法およびその方法をコンピュータに実行させるプログラム

(57) 【要約】

【課題】 プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減すること。

【解決手段】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワーク3-1と外部ネットワーク2との間でパケットの中継処理を行うネットワーク中継装置7において、プライベートネットワーク3-1内から送信されたESPパケットをUDPパケットにカプセル化して外部ネットワーク2に中継する第1中継部と、外部ネットワーク2からのUDPパケットをESPパケットにデカプセル化してプライベートネットワーク3-1内に中継する第2中継部とを備える。



【特許請求の範囲】

【請求項 1】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置において、

前記プライベートネットワーク内から送信された ESP パケットを UDP パケットにカプセル化して前記プライベートネットワーク外に中継する第 1 中継手段と、
前記プライベートネットワーク外からの UDP パケットを ESP パケットにデカプセル化して前記プライベートネットワーク内に中継する第 2 中継手段と、
を具備することを特徴とするネットワーク中継装置。

【請求項 2】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置された IPsec 装置と、を備えたデータ通信システムにおいて、

前記ネットワーク中継装置は、
前記プライベートネットワーク内から送信された ESP パケットを UDP パケットにカプセル化して前記 IPsec 装置宛てに中継する第 1 中継手段と、
前記 IPsec 装置からの UDP パケットを ESP パケットにデカプセル化して前記プライベートネットワーク内に中継する第 2 中継手段と、
を具備し、
前記 IPsec 装置は、
前記第 1 中継手段からの前記 UDP パケットを ESP パケットにデカプセル化するデカプセル化手段と、
前記デカプセル化手段がデカプセル化した前記 ESP パケットの受信処理を行う ESP 受信処理手段と、
前記プライベートネットワークに ESP パケットを送信する場合、該 ESP パケットを UDP パケットにカプセル化して送信する送信手段と、
を具備することを特徴とするデータ通信システム。

【請求項 3】 前記ネットワーク中継装置は、
前記第 1 中継手段がカプセル化する前記 ESP パケットの送信元の UDP ポート番号を決定する決定手段と、
前記送信元の前記プライベートアドレスおよび前記 UDP ポート番号を対応させて記憶する第 1 記憶手段と、
を具備し、
前記 IPsec 装置は、前記デカプセル化手段がデカプセル化する前記 UDP パケットの UDP 送信元ポート番号を記憶する第 2 記憶手段を具備し、
前記第 1 中継手段は、前記決定手段が決定した前記 UDP ポート番号を UDP 送信ポート番号として用いて前記カプセル化を行い、前記第 1 記憶手段が記憶した前記 UDP ポート番号を UDP 宛先ポート番号とする UDP パ

ケットを前記第 2 中継手段が受信した後、該 UDP ポート番号に対応する前記送信元からの前記 ESP パケットの前記カプセル化を省略し、

前記第 2 中継手段は、受信した前記 UDP パケットの UDP 宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、

前記送信手段は、前記第 2 記憶手段が記憶した前記 UDP 送信元ポート番号を UDP 宛先ポート番号として用いて前記カプセル化を行うことを特徴とする請求項 2 に記載のデータ通信システム。

【請求項 4】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置された IPsec 装置と、を備えたデータ通信システムにおいて、

前記ネットワーク中継装置は、
前記プライベートネットワーク内から送信された IKE ネゴシエーション用の UDP パケットを前記 IPsec 装置宛てに中継する場合に該 UDP パケットの UDP 送信元ポート番号を決定して中継する第 1 中継手段と、
前記 UDP パケットの送信元の前記プライベートアドレスおよび前記 UDP 送信元ポート番号を対応させて記憶する第 1 記憶手段と、
前記 IPsec 装置からの UDP パケットを ESP パケットにデカプセル化し、該 UDP パケットの UDP 宛先ポート番号に対応する前記プライベートアドレス宛てに中継する第 2 中継手段と、

前記 IPsec 装置は、
前記第 1 中継手段からの前記 UDP パケットの前記 UDP 送信元ポート番号を記憶する第 2 記憶手段と、
前記プライベートネットワークに ESP パケットを送信する場合、前記第 2 記憶手段が記憶した前記 UDP 送信元ポート番号を UDP 宛先ポート番号として用い、該 ESP パケットを UDP パケットにカプセル化して送信する送信手段と、
を具備することを特徴とするデータ通信システム。

【請求項 5】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間で ESP パケットを送受信するデータ通信方法において、

前記プライベートネットワーク内から送信された ESP パケットを UDP パケットにカプセル化して前記プライベートネットワーク外に中継する第 1 中継工程と、
前記プライベートネットワーク外からの UDP パケットを ESP パケットにデカプセル化して前記プライベートネットワーク内に中継する第 2 中継工程と、
を含むことを特徴とするデータ通信方法。

【請求項6】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でESPパケットを送受信するデータ通信方法において、

前記プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化して前記プライベートネットワーク外に中継する第1中継工程と、

前記第1中継工程で中継された前記UDPパケットの宛先側で、該UDPパケットをESPパケットにデカプセル化するデカプセル化工程と、

前記デカプセル化工程でデカプセル化された前記ESPパケットの受信処理を行うESP受信処理工程と、

前記宛先側で、前記プライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信する送信工程と、

前記送信工程で送信された前記UDPパケットをESPパケットにデカプセル化して前記プライベートネットワーク内に中継する第2中継工程と、

を含むことを特徴とするデータ通信方法。

【請求項7】 前記第1中継工程では、前記ESPパケットの送信元のUDPポート番号を決定し、該UDPポート番号をUDP送信元ポート番号として用いて前記カプセル化を行い、該送信元の前記プライベートアドレスおよび該UDPポート番号を対応させて記憶し、該UDPポート番号をUDP宛先ポート番号とするUDPパケットが前記第2中継工程で受信された後、該UDPポート番号に対応する前記送信元からの前記ESPパケットの前記カプセル化を省略し、

前記第2中継工程では、受信した前記UDPパケットのUDP宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、

前記デカプセル化工程では、前記デカプセル化する前記UDPパケットのUDP送信元ポート番号を記憶し、

前記送信工程では、前記デカプセル化工程で記憶された前記UDP送信元ポート番号をUDP宛先ポート番号として用いて前記カプセル化を行うことを特徴とする請求項6に記載のデータ通信方法。

【請求項8】 自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でESPパケットを送受信するデータ通信方法において、

前記プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットを該プライベートネットワーク外に中継する場合、該UDPパケットのUDP送信元ポート番号を決定し、該UDPパケットの送信元の前記プライベートアドレスおよび該UDP送信元ポート番号を対応させて記憶する第1中継工程と、

前記第1中継工程で中継された前記UDPパケットの宛

先側で、該UDPパケットの前記UDP送信元ポート番号を記憶する記憶工程と、

前記宛先側で、前記プライベートネットワークにESPパケットを送信する場合、前記記憶工程で記憶された前記UDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信する送信工程と、

前記送信工程で送信された前記UDPパケットをESPパケットにデカプセル化し、該UDPパケットの前記UDP宛先ポートに対応する前記プライベートアドレス宛てに中継する第2中継工程と、

を含むことを特徴とするデータ通信方法。

【請求項9】 請求項5～8のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、プライベートなアドレスを用いるプライベートネットワークとプライベートネットワーク外の外部ネットワークとの間でIPSec通信を行うネットワーク中継装置、データ通信システム、データ通信方法およびその方法をコンピュータに実行させるプログラムに関する。

【0002】

【従来の技術】IP (Internet Protocol) による通信では、ネットワーク上の各装置に対して固有のIPアドレスを割り付け、これらのIPアドレスを各装置の識別子として用いる。詳細には、送信データ内のIPヘッダに宛先および送信元のIPアドレス情報を格納することによって、データを正しい宛先に転送するとともにデータの送信元を通知する。インターネット (The Internet) 等のパブリックな開かれたネットワークでは、IPアドレスが重複しないように、全世界で唯一となるグローバルIPアドレスが使用される。

【0003】しかし、プライベートな閉じたネットワーク (以下、プライベートネットワークと呼ぶ) では、グローバルIPアドレスを節約するために、該プライベートネットワーク内でのみ重複しないプライベートIPアドレスを使用することができる。プライベートネットワークでは、インターネット等の外部のネットワークとの通信を行う場合、TCP (Transmission Control Protocol) /UDP (User Datagram Protocol) およびNAT (Network Address Translator) を用い、プライベートネットワークに対して一つ割り当てられたグローバルIPアドレスとプライベートIPアドレスとのアドレス変換を行う。

【0004】プライベートネットワーク内の装置から外部のネットワークにデータを送信する場合、プライベートネットワークと外部のネットワークとを接続するルータは、中継するデータの送信元IPアドレスをプライベートIPアドレスからグローバルIPアドレスに変換す

10

20

30

40

50

る。また、ルータは、使用中でないTCP/UDPポート番号（以下、単にポート番号と呼ぶ）をポート番号プールから選択して送信元ポート番号として決定し、中継データの変換前の送信元ポート番号を、決定した送信元ポート番号に変換する。そして、ルータは、これらのプライベートIPアドレス、変換元ポート番号（変換前の送信元ポート番号）および変換後ポート番号（変換後の送信元ポート番号）を対応させて変換テーブルに保持しておく。

【0005】一方、外部のネットワークからプライベートネットワーク内の装置にデータを送信する場合、ルータは、中継データの宛先ポート番号および変換テーブルに基づいて、その宛先ポート番号に一致する変換後ポート番号に対応するプライベートIPアドレスおよび変換元ポート番号を検索し、中継データのグローバルIPアドレスおよび宛先ポート番号を検索結果のプライベートIPアドレスおよび変換元ポート番号に変換する。このように、一つのグローバルIPアドレスを用いてプライベートネットワーク内の各装置とプライベートネットワーク外との通信を行っている。

【0006】ところで、IPのセキュリティ・プロトコルとして、IPSec（IP Security Protocol）が知られている。IPSecの暗号・認証プロトコルであるESP（IP Encapsulating Security Payload）は、TCP/UDPと同じトランスポート層のプロトコルであって、TCP/UDPを使用せず、ポート番号によるアドレス変換を行わない。すなわち、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行うことができないという不具合がある。

【0007】この不具合を解決する従来の通信方法として、プライベートネットワーク内の各IPSec装置（IPSec通信を行う装置）がESPパケットをUDPパケットにカプセル化して送信する通信方法が知られている。この通信方法では、プライベートネットワーク内の各IPSec装置に対し、ESPパケットをUDPパケットにカプセル化させるプログラムをユーザがインストールし、このプログラムに従って各IPSec装置がESPパケットをUDPパケットにカプセル化して送信する。これにより、ポート番号によるアドレス変換がルータで可能になり、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信が可能となる。

【0008】

【発明が解決しようとする課題】しかしながら、上述した技術によれば、プライベートネットワーク内の各IPSec装置がESPパケットをUDPパケットにカプセル化するため、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装に手間がかかり、また、IPSec装置ごとに該機能の管理を行わなければならない、コストが上昇するという

問題点があった。

【0009】この発明は上記に鑑みてなされたものであって、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減することを目的とする。

【0010】

【課題を解決するための手段】上記の目的を達成するために、請求項1にかかるネットワーク中継装置は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置において、前記プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化して前記プライベートネットワーク外に中継する第1中継手段と、前記プライベートネットワーク外からのUDPパケットをESPパケットにデカプセル化して前記プライベートネットワーク内に中継する第2中継手段と、を具備するものである。

【0011】この請求項1のネットワーク中継装置にあっては、第1中継手段が、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してプライベートネットワーク外に中継し、第2中継手段が、プライベートネットワーク外からのUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESPパケット/UDPパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができる。

【0012】また、請求項2にかかるデータ通信システムは、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたIPSec装置と、を備えたデータ通信システムにおいて、前記ネットワーク中継装置は、前記プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化して前記IPSec装置宛てに中継する第1中継手段と、前記IPSec装置からのUDPパケットをESPパケットにデカプセル化して前記プライベートネットワーク内に中継する第2中継手段と、を具備し、前記IPSec装置は、前記第1中継手段からの前記UDPパケットをESPパケットにデカプセル化するデカプセル化手段と、前記デカプセル化手段がデカプセル化した前記ESPパケットの受信処理を行うESP受信処理手段と、前記プライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信する送信手段と、を具備するものである。

【0013】この請求項2のデータ通信システムにおいては、第1中継手段が、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してIPSec装置宛てに中継し、第2中継手段が、IPSec装置からのUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継し、デカプセル化手段が、第1中継手段からのUDPパケットをESPパケットにデカプセル化し、ESP受信処理手段が、デカプセル化手段がデカプセル化したESPパケットの受信処理を行い、送信手段が、プライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信する。これにより、ESPパケット/UDPパケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめて行うことができる。

【0014】また、請求項3にかかるデータ通信システムは、請求項2に記載のデータ通信システムにおいて、前記ネットワーク中継装置が、前記第1中継手段がカプセル化する前記ESPパケットの送信元のUDPポート番号を決定する決定手段と、前記送信元の前記プライベートアドレスおよび前記UDPポート番号を対応させて記憶する第1記憶手段と、を具備し、前記第1中継手段が、前記決定手段が決定した前記UDPポート番号をUDP送信ポート番号として用いて前記カプセル化を行い、前記第1記憶手段が記憶した前記UDPポート番号をUDP宛先ポート番号とするUDPパケットを前記第2中継手段が受信した後、該UDPポート番号に対応する前記送信元からの前記ESPパケットの前記カプセル化を省略し、前記第2中継手段が、受信した前記UDPパケットのUDP宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、前記IPSec装置が、前記デカプセル化手段がデカプセル化する前記UDPパケットのUDP送信元ポート番号を記憶する第2記憶手段を具備し、前記送信手段が、前記第2記憶手段が記憶した前記UDP送信元ポート番号をUDP宛先ポート番号として用いて前記カプセル化を行うものである。

【0015】この請求項3のデータ通信システムにおいては、決定手段が、第1中継手段がカプセル化するESPパケットの送信元のUDPポート番号を決定し、第1記憶手段が、送信元のプライベートアドレスおよびUDPポート番号を対応させて記憶し、第1中継手段が、決定手段が決定したUDPポート番号をUDP送信ポート番号として用いてカプセル化を行い、第1記憶手段が記憶したUDPポート番号をUDP宛先ポート番号とするUDPパケットを第2中継手段が受信した後、該UDPポート番号に対応する送信元からのESPパケットのカプセル化を省略し、第2中継手段が、受信したUDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、第2記憶手段が、デカプセ

ル化手段がデカプセル化するUDPパケットのUDP送信元ポート番号を記憶し、送信手段が、第2記憶手段が記憶したUDP送信元ポート番号をUDP宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのESPパケットのカプセル化を2回目以降省略して、UDPパケットへのカプセル化によるオーバーヘッドを低減することができる。

【0016】また、請求項4にかかるデータ通信システムは、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でパケットの中継処理を行うネットワーク中継装置と、前記プライベートネットワーク外に配置されたIPSec装置と、を備えたデータ通信システムにおいて、前記ネットワーク中継装置は、前記プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットを前記IPSec装置宛てに中継する場合に該UDPパケットのUDP送信元ポート番号を決定して中継する第1中継手段と、前記UDPパケットの送信元の前記プライベートアドレスおよび前記UDP送信元ポート番号を対応させて記憶する第1記憶手段と、前記IPSec装置からのUDPパケットをESPパケットにデカプセル化し、該UDPパケットのUDP宛先ポート番号に対応する前記プライベートアドレス宛てに中継する第2中継手段と、前記IPSec装置は、前記第1中継手段からの前記UDPパケットの前記UDP送信元ポート番号を記憶する第2記憶手段と、前記プライベートネットワークにESPパケットを送信する場合、前記第2記憶手段が記憶した前記UDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信する送信手段と、を具備するものである。

【0017】この請求項4のデータ通信システムにおいては、第1中継手段が、プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットをIPSec装置宛てに中継する場合に該UDPパケットのUDP送信元ポート番号を決定して中継し、第1記憶手段が、UDPパケットの送信元のプライベートアドレスおよびUDP送信元ポート番号を対応させて記憶し、第2中継手段が、IPSec装置からのUDPパケットをESPパケットにデカプセル化し、該UDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継し、第2記憶手段が、第1中継手段からのUDPパケットのUDP送信元ポート番号を記憶し、送信手段が、プライベートネットワークにESPパケットを送信する場合、第2記憶手段が記憶したUDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信する。これにより、UDPパケットからESPパケットへのデカプセル化をネットワーク中継装置でまとめて

行うことができ、また、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化する必要がなくなる。

【0018】また、請求項5にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でESPパケットを送受信するデータ通信方法において、前記プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化して前記プライベートネットワーク外に中継する第1中継工程と、前記プライベートネットワーク外からのUDPパケットをESPパケットにデカプセル化して前記プライベートネットワーク内に中継する第2中継工程と、を含むものである。

【0019】この請求項5のデータ通信方法にあっては、第1中継工程で、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してプライベートネットワーク外に中継し、第2中継工程で、プライベートネットワーク外からのUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESPパケット/UDPパケットのカプセル化およびデカプセル化をまとめて行うことができる。

【0020】また、請求項6にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でESPパケットを送受信するデータ通信方法において、前記プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化して前記プライベートネットワーク外に中継する第1中継工程と、前記第1中継工程で中継された前記UDPパケットの宛先側で、該UDPパケットをESPパケットにデカプセル化するデカプセル化工程と、前記デカプセル化工程でデカプセル化された前記ESPパケットの受信処理を行うESP受信処理工程と、前記宛先側で、前記プライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信する送信工程と、前記送信工程で送信された前記UDPパケットをESPパケットにデカプセル化して前記プライベートネットワーク内に中継する第2中継工程と、を含むものである。

【0021】この請求項6のデータ通信方法にあっては、第1中継工程で、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してプライベートネットワーク外に中継し、デカプセル化工程で、第1中継工程で中継されたUDPパケットの宛先側で該UDPパケットをESPパケットにデカプセル化し、ESP受信処理工程で、デカプセル化工程で

デカプセル化されたESPパケットの受信処理を行い、送信工程で、宛先側からプライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信し、第2中継工程で、送信工程で送信されたUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESPパケット/UDPパケットのカプセル化およびデカプセル化をまとめて行うことができる。

【0022】また、請求項7にかかるデータ通信方法は、請求項6に記載のデータ通信方法において、前記第1中継工程では、前記ESPパケットの送信元のUDPポート番号を決定し、該UDPポート番号をUDP送信元ポート番号として用いて前記カプセル化を行い、該送信元の前記プライベートアドレスおよび該UDPポート番号を対応させて記憶し、該UDPポート番号をUDP宛先ポート番号とするUDPパケットが前記第2中継工程で受信された後、該UDPポート番号に対応する前記送信元からの前記ESPパケットの前記カプセル化を省略し、前記第2中継工程では、受信した前記UDPパケットのUDP宛先ポート番号に対応する前記プライベートアドレス宛てに前記中継を行い、前記デカプセル化工程では、前記デカプセル化する前記UDPパケットのUDP送信元ポート番号を記憶し、前記送信工程では、前記デカプセル化工程で記憶された前記UDP送信元ポート番号をUDP宛先ポート番号として用いて前記カプセル化を行うものである。

【0023】この請求項7のデータ通信方法にあっては、第1中継工程で、ESPパケットの送信元のUDPポート番号を決定し、該UDPポート番号をUDP送信元ポート番号として用いてカプセル化を行い、該送信元のプライベートアドレスおよび該UDPポート番号を対応させて記憶し、該UDPポート番号をUDP宛先ポート番号とするUDPパケットが第2中継工程で受信された後、該UDPポート番号に対応する送信元からのESPパケットのカプセル化を省略し、第2中継工程で、受信したUDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、デカプセル化工程で、デカプセル化するUDPパケットのUDP送信元ポート番号を記憶し、送信工程で、デカプセル化工程で記憶されたUDP送信元ポート番号をUDP宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのESPパケットのカプセル化を2回目以降省略して、UDPパケットへのカプセル化によるオーバーヘッドを低減することができる。

【0024】また、請求項8にかかるデータ通信方法は、自プライベートネットワーク内でユニークなプライベートアドレスを用いるプライベートネットワークと該プライベートネットワーク外の外部ネットワークとの間でESPパケットを送受信するデータ通信方法におい

て、前記プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットを該プライベートネットワーク外に中継する場合、該UDPパケットのUDP送信元ポート番号を決定し、該UDPパケットの送信元の前記プライベートアドレスおよび該UDP送信元ポート番号を対応させて記憶する第1中継工程と、前記第1中継工程で中継された前記UDPパケットの宛先側で、該UDPパケットの前記UDP送信元ポート番号を記憶する記憶工程と、前記宛先側で、前記プライベートネットワークにESPパケットを送信する場合、前記記憶工程で記憶された前記UDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信する送信工程と、前記送信工程で送信された前記UDPパケットをESPパケットにデカプセル化し、該UDPパケットの前記UDP宛先ポートに対応する前記プライベートアドレス宛てに中継する第2中継工程と、を含むものである。

【0025】この請求項8のデータ通信方法にあっては、第1中継工程で、プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットを該プライベートネットワーク外に中継する場合、該UDPパケットのUDP送信元ポート番号を決定し、該UDPパケットの送信元のプライベートアドレスおよび該UDP送信元ポート番号を対応させて記憶し、記憶工程で、第1中継工程で中継されたUDPパケットの宛先側で、該UDPパケットのUDP送信元ポート番号を記憶し、送信工程で、宛先側からプライベートネットワークにESPパケットを送信する場合、記憶工程で記憶されたUDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信し、第2中継工程で、送信工程で送信されたUDPパケットをESPパケットにデカプセル化し、該UDPパケットのUDP宛先ポートに対応するプライベートアドレス宛てに中継する。これにより、UDPパケットからESPパケットへのデカプセル化をまとめて行うことができ、また、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化する必要がなくなる。

【0026】また、請求項9にかかるプログラムは、請求項5～8のいずれか一つに記載された方法をコンピュータに実行させるものである。これにより、請求項5～8のいずれか一つに記載された方法の動作をコンピュータによって実現することが可能となる。

【0027】ここで、「プログラム」とは、データ処理方法を記述したものであって、記述する言語や記述方法は特に限定されず、ソースコード、バイナリコード、実行形式等の形式を問わない。なお、「プログラム」は必ずしも単一に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、OS等の別個のプログラムと協働してその機能を達成するもの

を含む。

【0028】

【発明の実施の形態】以下に、この発明の実施の形態を、添付の図面を参照して詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。図1は、この発明の一実施の形態にかかる通信ネットワークのシステム構成を示す説明図である。この実施の形態の通信ネットワークは、センタネットワーク1と、複数のプライベートネットワーク3-1～3-N1と、センタネットワーク1およびプライベートネットワーク3-1～3-N1を接続するインターネット等の外部ネットワーク2とを備える。外部ネットワーク2は、全世界の不特定多数のネットワークと繋がるグローバル・ネットワークである。

【0029】各プライベートネットワーク3-1～3-N1は、全て同様の構成であって、外部ネットワーク2に接続するルータと、複数のIPSec装置とを有する。各IPSec装置は、自プライベートネットワーク内でのみユニークなプライベートIPアドレスを用いて通信を行う。各プライベートネットワークは、グローバルIPアドレスを一つ有する。この例では、プライベートネットワーク3-1が、ルータ7（グローバルIPアドレスG11、プライベートIPアドレスP-0）とIPSec装置8-1～8-N2（プライベートIPアドレスP-1～P-N2）とを備える。

【0030】ただし、N1およびN2は、任意の数である。センタネットワーク1は、センタネットワーク1外の装置によるアクセスを受けるデータベース・サーバ等のサーバ4（グローバルIPアドレスG1）と、外部ネットワーク2に接続するルータ6と、ルータ6（グローバルIPアドレスG3）とサーバ4との間に設けたIPSec装置5（グローバルIPアドレスG2）とを備える。

【0031】たとえば、IPSec装置5とIPSec装置8-1とがIPSec通信を行う場合、まず、暗号鍵交換を行うIKE（Internet Key Exchange）ネゴシエーションをこれらのIPSec装置間で行い、その後、ESPプロトコルに基づいて、IPSec装置8-1からIPSec装置5宛てにESPパケットを送信し、IPSec装置5からIPSec装置8-1宛てにESPパケットを送信する。なお、端末装置であるIPSec装置8-1～8-N2に代えて、中継装置であるIPSec装置を設け、各IPSec装置に複数の端末装置を接続してもよい。また、センタネットワークを複数設けてもよいし、各センタネットワーク内に複数のサーバを設けてもよい。

【0032】つぎにルータ7の機能構成について説明する。図2は、図1に示したルータ7の機能構成を示すブロック図である。ルータ7は、外部ネットワーク2との通信を行うインターフェース部11と、プライベートネ

ットワーク 3-1 内から送信された ESP パケットを UDP パケットにカプセル化して外部ネットワーク 2 に中継する第 1 中継部 12 と、この発明の NAT 変換に用いる変換情報を記憶する記憶部 13 と、外部ネットワーク 2 からの UDP パケットを ESP パケットにデカプセル化してプライベートネットワーク 3-1 内に中継する第 2 中継部 14 と、プライベートネットワーク 3-1 内との通信を行うインターフェース部 15 とを備える。

【0033】第 1 中継部 12 は、UDP パケットの送信元 UDP ポート番号（以下、単に送信元ポート番号と呼ぶ）を決定する決定部 16 を有し、プライベートネットワーク 3-1 内の IP Sec 装置 8-1 ~ 8-N2 からの ESP パケットを UDP パケットにカプセル化して外部ネットワーク 2 に中継する。また、第 1 中継部 12 は、決定部 16 が決定した送信元ポート番号と ESP パケットの送信元プライベート IP アドレスとを対応させた変換情報を記憶部 13 に格納する。記憶部 13 は、ハードディスク等の記録媒体を有し、変換情報を記憶する。第 2 中継部 14 は、記憶部 13 の変換情報を参照し、外部ネットワーク 2 からの UDP パケットを ESP

パケットにデカプセル化してプライベートネットワーク 3-1 内に中継する。
【0034】つぎに、IP Sec 装置 5 の機能構成について説明する。図 3 は、図 1 に示した IP Sec 装置 5 の機能構成を示すブロック図である。IP Sec 装置 5 は、センタネットワーク 1 内との通信を行うインターフェース部 21 と、ルータ 6 に接続するインターフェース部 27 と、外部ネットワーク 2 からの UDP パケットを ESP パケットにデカプセル化するデカプセル化部 24 と、デカプセル化部 24 がデカプセル化した ESP パケットの ESP 受信処理を行う ESP 受信処理部 22 と、センタネットワーク 1 内から送信されたオリジナル IP パケットを暗号化して ESP パケットを生成する ESP パケット生成部 23 と、ESP パケット生成部 23 が生成した ESP パケットを UDP パケットにカプセル化して外部ネットワーク 2 に送信する送信部 26 と、この発明の NAT 変換に用いる変換情報を記憶する記憶部 25 とを備える。

【0035】デカプセル化部 24 は、外部ネットワーク 2 からの UDP パケットを受信すると、その UDP パケットの送信元ポート番号を変換情報として記憶部 25 に格納するとともに、その UDP パケットを ESP パケットにデカプセル化する。ESP 受信処理部 22 は、デカプセル化部 24 がデカプセル化した ESP パケットの ESP 受信処理を行う。すなわち、ESP 受信処理部 22 は、ESP パケットに含まれる暗号化されたオリジナル IP パケットを復号化し、復号化されたオリジナル IP パケットをセンタネットワーク 1 内に送信する。

【0036】ESP パケット生成部 23 は、センタネットワーク 1 内のサーバ 4 からのオリジナル IP パケッ

トを暗号化して ESP パケットを生成する。送信部 26 は、記憶部 25 の変換情報を参照し、ESP パケット生成部 23 が生成した ESP パケットを UDP パケットにカプセル化して外部ネットワーク 2 に送信する。記憶部 25 は、ハードディスク等の記録媒体を有し、変換情報を記憶する。なお、この例では、ルータ 7 に ESP パケット/UDP パケットのカプセル化およびデカプセル化の機能を持たしているが、ルータ 7 と IP Sec 装置 8-1 ~ 8-N2 との間に該機能を達成する装置を設けてもよい。また、この例では、IP Sec 装置 5 とルータ 6 とを別体に設けているが、これらを一体に設けてもよい。また、IP Sec 装置 5 とサーバ 4 とを一体に設けてもよい。

【0037】さて、これまで、ルータ 7 および IP Sec 装置 5 の構成について説明したが、ルータ 7 および IP Sec 装置 5 の各構成要素は機能概念的なものであり、必ずしも物理的に図示したように構成されていなくてもよい。たとえば、ルータ 7 および IP Sec 装置 5 が備える処理機能のうち全部または一部を、図示しない CPU (Central Processing Unit) およびこの CPU にて解釈実行されるプログラムによって実現することができる。すなわち、図示しない ROM には、OS (Operating System) 等と協働して CPU に命令を与え、CPU に各種処理を行わせるコンピュータプログラムが格納されている。そして、CPU は、このプログラムに従って各種処理を行う。また、ルータ 7 および IP Sec 装置 5 が備える処理機能のうち全部または一部を、ワイヤードロジックによるハードウェアとして実現することも可能である。

【0038】以上の構成において、この実施の形態の動作についてフローチャートを参照して説明する。図 4 は、この実施の形態にかかるルータ 7 が外部ネットワーク 2 にパケットを送信する場合の動作手順を示すフローチャートである。ルータ 7 では、プライベートネットワーク 3-1 内から送信されたプライベートネットワーク 3-1 外宛てのパケットをインターフェース部 15 が受信すると、まず、第 1 中継部 12 が、そのパケットが ESP パケットであるか否かを判定する (S1)。図 5 は、プライベートネットワーク内の IP Sec 装置が送信する ESP パケットを含む IP パケットの一例を示す説明図である。

【0039】ここでは、IP Sec 装置 8-1 によるサーバ 4 宛てのパケットの例を示している。このパケットでは、オリジナル IP パケットを暗号化し、ESP ヘッダを付加し、さらに IP ヘッダを付加している。この IP ヘッダの宛先アドレスは、IP Sec 装置 5 のグローバル IP アドレスであり、送信元アドレスは IP Sec 装置 3-1 のプライベート IP アドレスである。なお、ここでは、オリジナル IP パケットの送信元アドレスとして IP Sec 装置 8-1 のプライベート IP アドレス

10

20

30

40

50

P-1を用いているが、プライベートIPアドレスをプライベートネットワーク3-1の外部に出したくない場合は、プライベートIPアドレスに代えて他の識別子を用いてもよい。

【0040】ステップS1で、受信パケットがESPパケットである場合、第1中継部12は、そのESPパケットを含むIPパケットのIPヘッダから、送信元アドレスとして格納されているプライベートIPアドレスを取得し、記憶部13を参照し、そのプライベートIPアドレスを含む変換情報が記憶されているか否かを判定する(S2)。図6は、この実施の形態にかかる変換情報の一例を示す説明図である。図6に示すように、変換情報は、ESPパケットの送信元のプライベートIPアドレスと該送信元に割り当てられたポート番号(UDPポート番号)とを対応させたものである。この例では、プライベートIPアドレスP-1とポート番号X-1が対応し、プライベートIPアドレスP-2とポート番号X-2が対応する。

【0041】ステップS2で、受信パケットの送信元に対応する変換情報が記憶部13に記憶されていない場合、決定部16は、記憶部13に記憶されたNAT変換用のポート番号プールの中から使用中でないポート番号を選択し、該送信元のポート番号として決定する(S3)。つぎに、第1中継部12は、決定部16が決定したポート番号と送信元のプライベートIPアドレスとを対応させた変換情報を記憶部13に格納する(S4)。つぎに、第1中継部12は、受信パケットのIPヘッダのNAT変換を行う(S5)。すなわち、第1中継部12は、図7に示すように、IPヘッダの送信元アドレスを、プライベートIPアドレスからグローバルIPアドレスG11に変換する。

【0042】つぎに、第1中継部12は、予め取り決めたUDPパケットカプセル化処理用のポート番号X0をUDPヘッダの宛先ポート番号として用い、ステップS3で決定したポート番号をUDPヘッダの送信元ポート番号として用いて、受信IPパケットをUDPパケットにカプセル化する(S6)。つぎに、グローバルIPアドレスG11を送信元アドレスとし、グローバルIPアドレスG2を宛先アドレスとするIPヘッダをUDPパケットに付加し、図8に示すようなIPパケットを生成する(S7)。そして、生成したデータを、インターフェース部11を介して外部ネットワーク2に送信する(S8)。

【0043】一方、ステップS1で、受信パケットがESPパケットでなかった場合、第1中継部12は、前述した従来と同様のNAT変換処理を行い(S9)、ステップS8に進む。また、ステップS2で、受信したESPパケットの送信元に対応する変換情報がすでに記憶部13に記憶されていた場合、第1中継部12は、ステップS5と同様のIPヘッダのNAT変換処理を行い、ス

テップS8に進む。すなわち、プライベートネットワーク3-1内の同一のIPSec装置からのESPパケットを受信した場合、UDPパケットへのカプセル化を2回目以降は省略する。

【0044】あるいは、プライベートネットワーク3-1内のIPSec装置からのIPSec装置5宛てのパケットを一度中継し、IPSec装置5からプライベートネットワーク3-1内の該IPSec装置宛てのパケットを受信したあと、UDPパケットへのカプセル化の省略を行うようにしてもよい。この方法によれば、UDPパケットへのカプセル化を最初の一度だけ行えばよく、あとは省略できるため、IPヘッダの20バイトおよびUDPヘッダの8バイトのオーバーヘッドを低減することができる。

【0045】また、UDPパケットへのカプセル化を一度行ったあと、所定時間以上、その送信元のIPSec装置宛てまたは該IPSec装置からのESPパケットの中継がなかった場合、該IPSec装置に対応する変換情報を開放し、使用していたポート番号をポート番号プールに戻してもよい。これにより、変換情報用のメモリ領域を低減することができる。この場合、該IPSec装置が再びESPパケットをIPSec装置5宛てに送信するときに、再びポート番号の取得が行われる。

【0046】つぎに、IPSec装置5が外部ネットワーク2からのパケットを受信する場合の動作について説明する。図9は、この実施の形態にかかるIPSec装置5が外部ネットワーク2からのパケットを受信する場合の動作手順を示すフローチャートである。IPSec装置5では、外部ネットワーク2からのパケットをルータ6を介してインターフェース部27が受信すると、まず、デカプセル化部24が、自装置宛てのパケットか否かを判定する(S11)。受信パケットが自装置宛てであった場合、デカプセル化部24は、該パケットが宛先ポート番号X0のUDPパケットであるか否かを判定する(S12)。

【0047】受信パケットが宛先ポート番号X0のUDPパケットである場合、デカプセル化部24は、そのUDPパケットをESPパケットにデカプセル化する(S13)。すなわち、デカプセル化部24は、受信パケットのIPヘッダおよびUDPヘッダを取り除く。つぎに、デカプセル化部24は、UDPヘッダの送信元ポート番号を取得し、該送信元ポートと送信元のIPSec装置とを対応させた変換情報(図10参照)を記憶部25に格納する(S14)。たとえば、図8に示したパケットを受信した場合は、送信元のIPSec装置8-1に対応させてポート番号X-1が記憶部25に格納される。プライベートネットワークのルータ側でポート番号の開放および再取得が行われた場合、デカプセル化部24は、記憶部25に記憶されている送信元IPSec装置のポート番号の情報を更新する。

【0048】また、記憶部25は、IPSec通信の相手装置情報として、相手装置であるIPSec装置のIPアドレスや受信ESP識別子等の情報を保持する(図11参照)。ESPヘッダには、IKEネゴシエーションでIPSec装置同士がお互いに決めた識別子が含まれている。この識別子によってESPパケットの送信元であるIPSec装置を識別することができる。つぎに、ESP受信処理部22は、ESPパケットに含まれる暗号化されたオリジナルIPパケットを復号化する(S15)。そして、ESP受信処理部22は、図12に示すようなオリジナルIPパケットをセンターネットワーク1内に送信する(S16)。

【0049】一方、ステップS11で、受信パケットが自装置宛でなかった場合、デカプセル化部24およびESP受信処理部22は、従来の通常の中継装置と同様の中継処理を行う(S17)。また、ステップS12で、受信パケットが宛先ポート番号X0のUDPパケットでなかった場合、デカプセル化部24およびESP受信処理部22は、受信パケットのプロトコルに応じた従来の通常の受信処理を行う(S18)。

【0050】つぎに、IPSec装置5が外部ネットワーク2にパケットを送信する場合の動作について説明する。図13は、この実施の形態にかかるIPSec装置5が外部ネットワーク2にパケットを送信する場合の動作手順を示すフローチャートである。IPSec装置5では、センターネットワーク1内から送信されたセンターネットワーク1外宛てのパケットをインターフェース部21が受信すると、まず、ESPパケット生成部23が、そのパケットがIPSec通信の対象であるか否かを判定する(S21)。

【0051】IPSec通信の対象であるか否かは、宛先IPアドレスや送信元IPアドレス等のパケットデータに基づいて判定する。記憶部25は、図14に示すような、宛先IPアドレス/マスク、送信元IPアドレス/マスク、TCP/UDP等のプロトコル、宛先ポート番号、送信元ポート番号、送信先装置等のIP通信対象となるパケットの条件を規定したIPSec通信対象パケット情報を保持する。ESPパケット生成部23は、IPSec通信対象パケット情報を参照し、受信パケットがIPSec通信対象パケット情報の条件を満たすか否かに基づいて、そのパケットがIPSec通信の対象であるか否かを判定する。

【0052】ステップS21で、受信パケットがIPSec通信の対象である場合、ESPパケット生成部23は、受信パケットであるオリジナルIPパケット(図15参照)を暗号化し、ESPヘッダを付加してESPパケットを生成する(S22)。つぎに、送信部26は、記憶部25を参照し、送信先のIPSec装置に対応する変換情報が記憶されているか否かを判定する(S23)。送信先のIPSec装置に対応する変換情報が記

憶されている場合、送信部26は、その変換情報のポート番号を取得して宛先ポート番号として用い、予め取り決めたポート番号X0を送信元ポート番号として用いて、ESPパケット生成部23が生成したESPパケットをUDPパケットにカプセル化する(S24)。

【0053】このように、IPSec装置5内でESPパケットの生成およびUDPパケットへのカプセル化をまとめて行うので、ESPパケットにIPヘッダを付加せずに直接UDPパケットにカプセル化することができる。つぎに、送信部26は、送信先のグローバルIPアドレスおよび自装置のグローバルIPアドレスG2の情報を含むIPヘッダをUDPパケットに付加し(S25)、図16に示すようなIPパケットを生成する。生成されたデータは、ルータ6を介して外部ネットワーク2に送信される(S26)。

【0054】一方、ステップS21で、受信パケットがIPSec通信の対象でなかった場合、ESPパケット生成部23および送信部26は、従来の通常の中継装置と同様のの中継処理を行い(S27)、ステップS26に進む。また、ステップS23で、送信先のIPSec装置に対応する変換情報が記憶部25に記憶されていない場合、ESPパケット生成部23および送信部26は、ESPパケットにIPヘッダを付加し(S28)、ステップS26に進む。

【0055】つぎに、ルータ7が外部ネットワーク2からのUDPパケットを受信する場合の動作について説明する。図17は、この実施の形態にかかるルータ7が外部ネットワーク2からのUDPパケットを受信する場合の動作手順を示すフローチャートである。ルータ7では、外部ネットワーク2からのUDPパケットをインターフェース部11が受信すると、まず、第2中継部14が、受信パケットの宛先ポート番号に対応する変換情報が記憶部13に記憶されているか否かを判定する(S31)。受信パケットの宛先ポート番号に対応する変換情報が記憶部13に記憶されている場合、第2中継部14は、受信パケットのIPヘッダおよびUDPヘッダを除去し、ESPパケットにデカプセル化する(S32)。

【0056】つぎに、第2中継部14は、受信パケットの宛先ポート番号に対応するプライベートIPアドレスを変換情報から取得し、このプライベートIPアドレスを送信先アドレスとするIPヘッダをESPパケットに付加する(S33)。たとえば、図16に示したパケットを受信した場合、第2中継部14は、そのパケットをESPパケットにデカプセル化し、宛先ポート番号X-1に対応するプライベートIPアドレスP-1を宛先アドレスとして用い、図18に示すIPパケットを生成する。そして、第2中継部14は、このIPパケットをプライベートネットワーク3-1内に送信する(S34)。

【0057】一方、ステップS31で、受信パケットの

10

20

30

40

50

宛先ポート番号に対応する変換情報が記憶部 25 に記憶されていない場合、第 2 中継部 14 は、前述した従来の NAT 変換処理を行い (S35)、ステップ S34 に進む。このように、UDP パケット / ESP パケットのカプセル化およびデカプセル化をルータ 7 が行うため、プライベートネットワーク内の IPsec 装置は標準の IPsec 処理を行うだけでプライベートネットワークの外部との IPsec 通信を行うことができる。

【0058】さて、前述した例では、プライベートネットワーク内の IPsec 装置によって 1 回目の ESP パケットを送信する場合に、送信元ポート番号を決定し、ESP パケットを UDP パケットにカプセル化していた。しかし、IKE ネゴシエーションで使用するパケットは UDP パケットであるので、IKE ネゴシエーションで使ったポート番号を、ESP パケットの送信元のポート番号として用いてもよい。すなわち、決定部 16 は、IKE ネゴシエーションで使用するポート番号を決定し、第 1 中継部 12 は、IKE ネゴシエーションで使ったポート番号およびプライベート IP アドレスを変換情報として記憶部 13 に格納する。

【0059】一方、IPsec 装置 5 のデカプセル化部 24 は、IKE ネゴシエーションで使ったポート番号を、IPsec 通信相手装置と対応させ、変換情報として記憶部 25 に格納する。これによって、プライベートネットワーク内の IPsec 装置がプライベートネットワーク外に ESP パケットを送信する場合、1 回目から UDP パケットへのカプセル化を省略することができる。また、前述した例では、センタネットワーク 1 内でグローバル IP アドレスを使用していたが、センタネットワーク 1 内でプライベート IP アドレスを使用してもよい。この場合は、ルータ 6 が NAT 変換を行う。

【0060】この実施の形態によれば、第 1 中継部 12 が、プライベートネットワーク 3-1 内から送信された ESP パケットを UDP パケットにカプセル化して外部ネットワーク 2 に中継し、第 2 中継部 14 が、外部ネットワーク 2 からの UDP パケットを ESP パケットにデカプセル化してプライベートネットワーク 3-1 内に中継する。これにより、ESP パケット / UDP パケットのカプセル化およびデカプセル化をルータ 7 でまとめることができるため、プライベートネットワーク 1 内とプライベートネットワーク 1 外との IPsec 通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【0061】なお、この実施の形態にかかる通信方法を実現するコンピュータプログラムを、フロッピー（登録商標）ディスク等の磁気ディスク、ROM、EPROM、EEPROM、フラッシュ ROM 等の半導体メモリ（カートリッジ、PC カード等に内蔵されているものを含む）、CD-ROM、DVD 等の光ディスク、MO 等の光磁気ディスク、等の可搬の記録媒体に格納し、この

記録媒体に記録されたプログラムを、ルータ 7 および IPsec 装置 5 に内蔵される ROM、RAM、ハードディスク等の固定用の記録媒体にインストールすることによって、そのルータ 7 および IPsec 装置 5 に前述した機能を具備させることもできる。

【0062】また、このプログラムを、LAN、WAN、インターネット等のネットワークを介して伝送し、伝送されたプログラムをルータ 7 および IPsec 装置 5 の固定用の記録媒体にインストールするようにしてもよい。また、このプログラムは、必ずしも単一に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されていてもよいし、OS 等の別個のプログラムと協働してその機能を達成するものであってもよい。

【0063】

【発明の効果】以上説明したように、この発明のネットワーク中継装置（請求項 1）は、第 1 中継手段が、プライベートネットワーク内から送信された ESP パケットを UDP パケットにカプセル化してプライベートネットワーク外に中継し、第 2 中継手段が、プライベートネットワーク外からの UDP パケットを ESP パケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESP パケット / UDP パケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめることができるため、プライベートネットワーク内とプライベートネットワーク外との IPsec 通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【0064】また、この発明のデータ通信システム（請求項 2）は、第 1 中継手段が、プライベートネットワーク内から送信された ESP パケットを UDP パケットにカプセル化して IPsec 装置宛てに中継し、第 2 中継手段が、IPsec 装置からの UDP パケットを ESP パケットにデカプセル化してプライベートネットワーク内に中継し、デカプセル化手段が、第 1 中継手段からの UDP パケットを ESP パケットにデカプセル化し、ESP 受信処理手段が、デカプセル化手段がデカプセル化した ESP パケットの受信処理を行い、送信手段が、プライベートネットワークに ESP パケットを送信する場合、該 ESP パケットを UDP パケットにカプセル化して送信する。これにより、ESP パケット / UDP パケットのカプセル化およびデカプセル化をネットワーク中継装置でまとめることができるため、プライベートネットワーク内とプライベートネットワーク外との IPsec 通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【0065】また、この発明のデータ通信システム（請求項 3）は、決定手段が、第 1 中継手段がカプセル化する ESP パケットの送信元の UDP ポート番号を決定し、第 1 記憶手段が、送信元のプライベートアドレスお

よびUDPポート番号を対応させて記憶し、第1中継手段が、決定手段が決定したUDPポート番号をUDP送信ポート番号として用いてカプセル化を行い、第1記憶手段が記憶したUDPポート番号をUDP宛先ポート番号とするUDPパケットを第2中継手段が受信した後、該UDPポート番号に対応する送信元からのESPパケットのカプセル化を省略し、第2中継手段が、受信したUDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、第2記憶手段が、デカプセル化手段がデカプセル化するUDPパケットのUDP送信元ポート番号を記憶し、送信手段が、第2記憶手段が記憶したUDP送信元ポート番号をUDP宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのESPパケットのカプセル化を2回目以降省略して、UDPパケットへのカプセル化によるオーバーヘッドを低減することができるため、通信効率を向上させることができる。

【0066】また、この発明のデータ通信システム（請求項4）は、第1中継手段が、プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットをIPSec装置宛てに中継する場合に該UDPパケットのUDP送信元ポート番号を決定して中継し、第1記憶手段が、UDPパケットの送信元のプライベートアドレスおよびUDP送信元ポート番号を対応させて記憶し、第2中継手段が、IPSec装置からのUDPパケットをESPパケットにデカプセル化し、該UDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継し、第2記憶手段が、第1中継手段からのUDPパケットのUDP送信元ポート番号を記憶し、送信手段が、プライベートネットワークにESPパケットを送信する場合、第2記憶手段が記憶したUDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信する。これにより、UDPパケットからESPパケットへのデカプセル化をネットワーク中継装置でまとめて行うことができ、また、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化する必要がなくなるため、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減することができる、また、通信効率を向上させることができる。

【0067】また、この発明のデータ通信方法（請求項5）は、第1中継工程で、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してプライベートネットワーク外に中継し、第2中継工程で、プライベートネットワーク外からのUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESPパケット／UDPパケットのカプセル化およびデカプセル

化をまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【0068】また、この発明のデータ通信方法（請求項6）は、第1中継工程で、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化してプライベートネットワーク外に中継し、デカプセル化工程で、第1中継工程で中継されたUDPパケットの宛先側で該UDPパケットをESPパケットにデカプセル化し、ESP受信処理工程で、デカプセル化工程でデカプセル化されたESPパケットの受信処理を行い、送信工程で、宛先側からプライベートネットワークにESPパケットを送信する場合、該ESPパケットをUDPパケットにカプセル化して送信し、第2中継工程で、送信工程で送信されたUDPパケットをESPパケットにデカプセル化してプライベートネットワーク内に中継する。これにより、ESPパケット／UDPパケットのカプセル化およびデカプセル化をまとめて行うことができるため、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減することができる。

【0069】また、この発明のデータ通信方法（請求項7）は、第1中継工程で、ESPパケットの送信元のUDPポート番号を決定し、該UDPポート番号をUDP送信元ポート番号として用いてカプセル化を行い、該送信元のプライベートアドレスおよび該UDPポート番号を対応させて記憶し、該UDPポート番号をUDP宛先ポート番号とするUDPパケットが第2中継工程で受信された後、該UDPポート番号に対応する送信元からのESPパケットのカプセル化を省略し、第2中継工程で、受信したUDPパケットのUDP宛先ポート番号に対応するプライベートアドレス宛てに中継を行い、デカプセル化工程で、デカプセル化するUDPパケットのUDP送信元ポート番号を記憶し、送信工程で、デカプセル化工程で記憶されたUDP送信元ポート番号をUDP宛先ポート番号として用いてカプセル化を行う。これにより、同一の送信元からのESPパケットのカプセル化を2回目以降省略して、UDPパケットへのカプセル化によるオーバーヘッドを低減することができるため、通信効率を向上させることができる。

【0070】また、この発明のデータ通信方法（請求項8）は、第1中継工程で、プライベートネットワーク内から送信されたIKEネゴシエーション用のUDPパケットを該プライベートネットワーク外に中継する場合、該UDPパケットのUDP送信元ポート番号を決定し、該UDPパケットの送信元のプライベートアドレスおよび該UDP送信元ポート番号を対応させて記憶し、記憶工程で、第1中継工程で中継されたUDPパケットの宛

先側で、該UDPパケットのUDP送信元ポート番号を記憶し、送信工程で、宛先側からプライベートネットワークにESPパケットを送信する場合、記憶工程で記憶されたUDP送信元ポート番号をUDP宛先ポート番号として用い、該ESPパケットをUDPパケットにカプセル化して送信し、第2中継工程で、送信工程で送信されたUDPパケットをESPパケットにデカプセル化し、該UDPパケットのUDP宛先ポートに対応するプライベートアドレス宛てに中継する。これにより、UDPパケットからESPパケットへのデカプセル化をまとめて行うことができ、また、プライベートネットワーク内から送信されたESPパケットをUDPパケットにカプセル化する必要がなくなるため、プライベートネットワーク内とプライベートネットワーク外とのIPSec通信を行う機能の実装および管理を容易化し、コストを低減することができ、また、通信効率を向上させることができる。

【0071】また、この発明のプログラム（請求項9）は、前述した発明にかかる方法の動作をコンピュータによって実現することが可能となる、という効果を奏する。

【図面の簡単な説明】

【図1】この発明の一実施の形態にかかる通信ネットワークのシステム構成を示す説明図である。

【図2】図1に示したルータの機能構成を示すブロック図である。

【図3】図1に示したIPSec装置の機能構成を示すブロック図である。

【図4】この実施の形態にかかるルータが外部ネットワークにパケットを送信する場合の動作手順を示すフローチャートである。

【図5】この実施の形態にかかるルータが受信するプライベートネットワーク内から送信されたIPパケットの一例を示す説明図である。

【図6】この実施の形態にかかるルータが記憶する変換情報の一例を示す説明図である。

【図7】この実施の形態にかかるIPヘッダのNAT変換後のIPパケットの一例を示す説明図である。

【図8】この実施の形態にかかるルータが外部ネットワークに送信するIPパケットの一例を示す説明図である。

【図9】この実施の形態にかかるIPSec装置が外部ネットワークからのパケットを受信する場合の動作手順

を示すフローチャートである。

【図10】この実施の形態にかかるIPSec装置が記憶する変換情報の一例を示す説明図である。

【図11】この実施の形態にかかるIPSec装置が記憶するIPSec通信相手装置情報の一例を示す説明図である。

【図12】この実施の形態にかかるIPSec装置がセンターネットワーク内に送信するIPパケットの一例を示す説明図である。

10 【図13】この実施の形態にかかるIPSec装置が外部ネットワークにパケットを送信する場合の動作手順を示すフローチャートである。

【図14】この実施の形態にかかるIPSec装置が記憶するIPSec通信対象パケット情報の一例を示す説明図である。

【図15】この実施の形態にかかるIPSec装置が受信するセンターネットワーク内から送信されたIPパケットの一例を示す説明図である。

20 【図16】この実施の形態にかかるIPSec装置が外部ネットワークに送信するIPパケットの一例を示す説明図である。

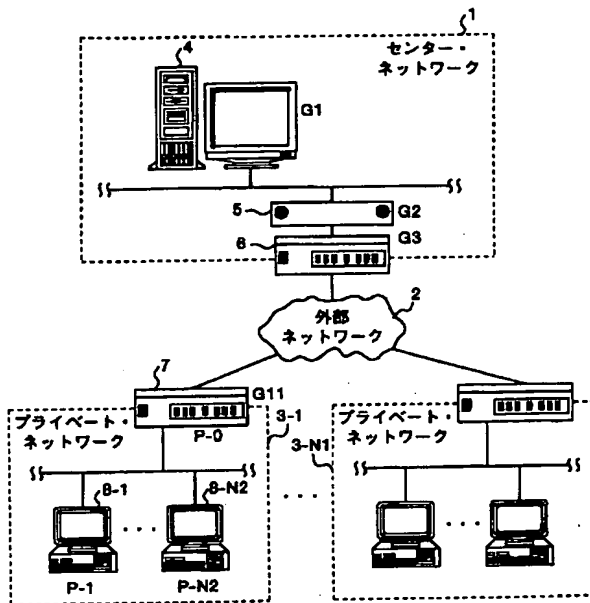
【図17】この実施の形態にかかるルータが外部ネットワークからのUDPパケットを受信する場合の動作手順を示すフローチャートである。

【図18】この実施の形態にかかるルータがプライベートネットワーク内に送信するIPパケットの一例を示す説明図である。

【符号の説明】

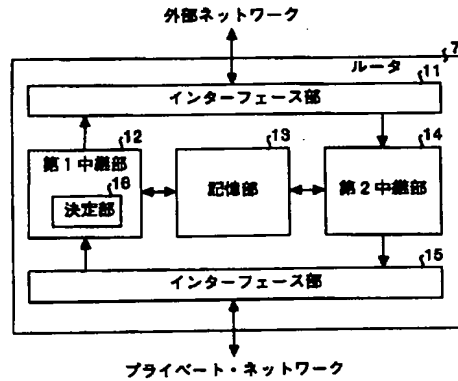
- 1 センターネットワーク
- 2 外部ネットワーク
- 3-1~3-N1 プライベートネットワーク
- 4 サーバ
- 5, 8-1~8-N2 IPSec装置
- 6, 7 ルータ
- 11, 15, 21, 27 インターフェース部
- 12 第1中継部
- 13, 25 記憶部
- 14 第2中継部
- 16 決定部
- 22 ESP受信処理部
- 23 ESPパケット生成部
- 24 デカプセル化部
- 26 送信部

【図1】



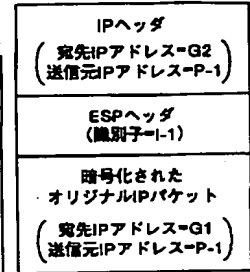
【図3】

【図2】



【図4】

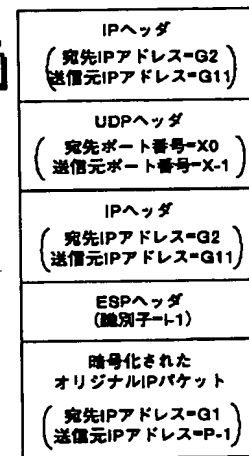
【図5】



【図6】

プライベートIP アドレス	ポート番号
P-1	X-1
P-2	X-2
...	...

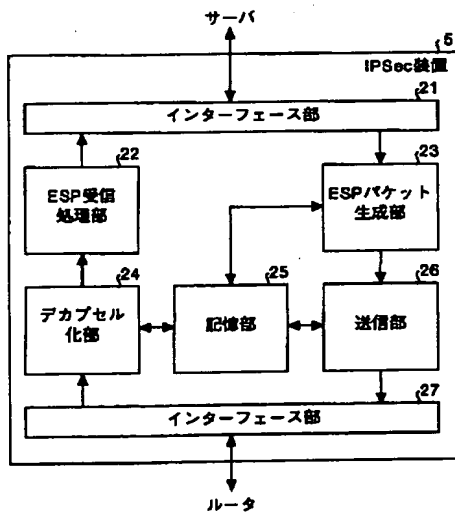
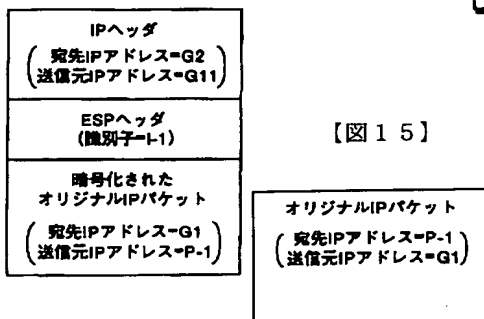
【図8】



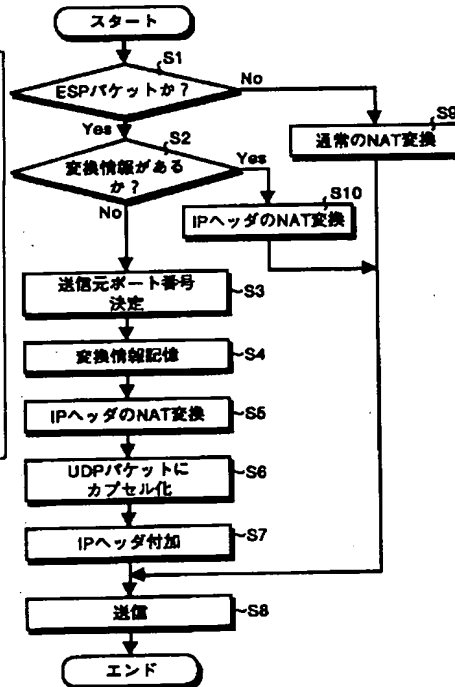
【図10】

送信元装置	UDP送信元 ポート番号
IPSec装置8-1	X-1
IPSec装置8-2	X-2
...	...

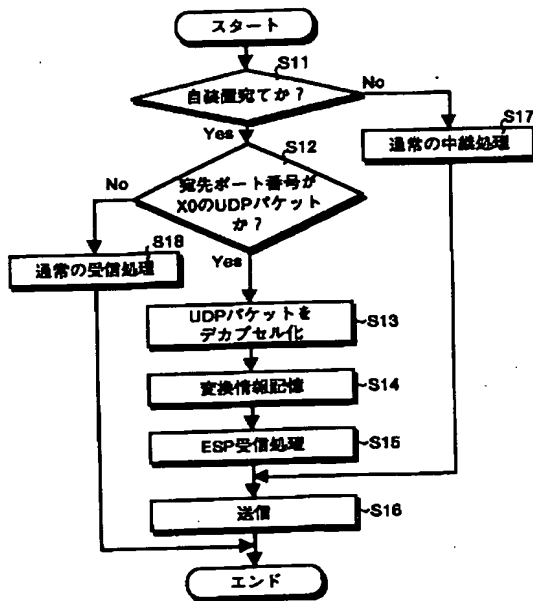
【図15】



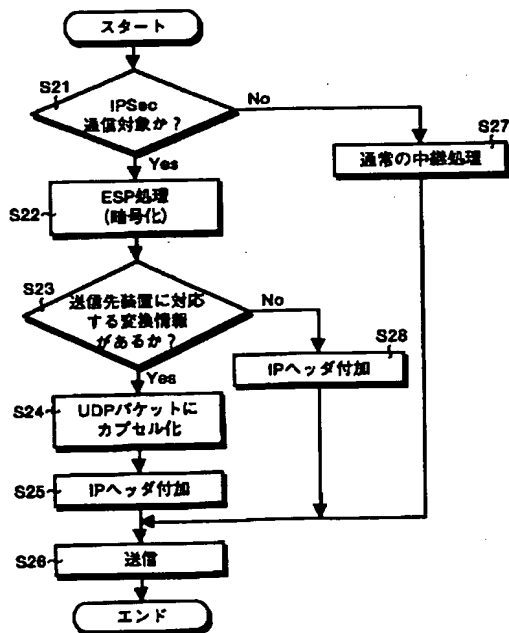
【図7】



【図 9】



【図 13】



【図 11】

相手装置	IPアドレス	識別子
IPSec装置8-1	G1	I-1
IPSec装置8-2	G1	I-2
⋮	⋮	⋮

【図 12】

オリジナルIPパケット (宛先IPアドレス=G1 送信元IPアドレス=P-1)

【図 18】

IPヘッダ (宛先IPアドレス=P-1 送信元IPアドレス=G2)
ESPヘッダ
暗号化された オリジナルIPパケット (宛先IPアドレス=P-1 送信元IPアドレス=G1)

【図 14】

宛先IPアドレス /マスク	送信元IPアドレス /マスク	プロトコル	宛先 ポート番号	送信元 ポート番号	送信先装置
IPa	IPb	all	all	all	IPSec 装置8-1
IPc	IPd	P-1	P-2	yy	IPSec 装置8-2
⋮	⋮	⋮	⋮	⋮	⋮

【図 16】

IPヘッダ (宛先IPアドレス=G11 送信元IPアドレス=G2)
UDPヘッダ (宛先ポート番号=X-1 送信元ポート番号=X0)
ESPヘッダ
暗号化された オリジナルIPパケット (宛先IPアドレス=P-1 送信元IPアドレス=G1)

【図 17】

